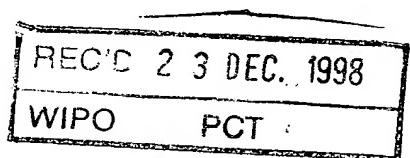


BUNDESREPUBLIK DEUTSCHLAND

DE98/2808

**PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

09/509401

Bescheinigung

Die ROBERT BOSCH GMBH in Stuttgart/Deutschland hat eine
Patentanmeldung unter der Bezeichnung

"Verfahren zum Zuordnen einer Fernbedienung zu
einer Basisstation"

am 26. September 1997 beim Deutschen Patent- und Markenamt
eingereicht.

Die angehefteten Stücke sind eine richtige und genaue
Wiedergabe der ursprünglichen Unterlagen dieser Patent-
anmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig
das Symbol G 08 C 17/02 der Internationalen Patentklassifikation
erhalten.

München, den 10. Dezember 1998

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Patentzeichen: 197 42 495.3

Sleek

18.08.97 Ba/Wt

5

ROBERT BOSCH GMBH, 70442 Stuttgart

10 Vefahren zum Zuordnen einer Fernbedienung zu einer
Basisstation

15 Stand der Technik

15 Die Erfindung geht aus von einem Verfahren nach der Gattung des Hauptanspruchs, wie es in der Deutschen Patentanmeldung AZ: 196 45 769.6 beschrieben ist. Danach erfolgt die Zuordnung einer Fernbedienung zu einer in einem Kraftfahrzeug angeordneten Basisstation, indem letztere ein Suchsignal absetzt, worauf im Reichweitenbereich des Suchsignales befindliche Fernbedienungen durch Rücksenden eines Kontaktsignales zu für die Fernbedienungen charakteristischen Zeitpunkten antworten. Durch Auswertung der Eingangszeitpunkte der Kontaktsignalrückmeldungen ermittelt die Basisstation die anwesenden Fernbedienungen. Eine davon wählt sie aus, und führt mit ihr eine „Challenge-Response“-Verifikation durch. Weil eine eindeutige Fernbedienungserkennung bereits durch Austausch von nur einem Signal möglich ist, und das Signal, da es nicht sicherheitsrelevant ist, einfach aufgebaut sein kann, erfolgt die gesamte Erkennung sehr schnell. Bestimmend für die Zuordnungsgeschwindigkeit ist daher vor allem die nachfolgende Challenge-Response-Verifikation. Sie basiert auf der Durchführung von sicherheitsrelevanten Rechenoperationen, die umfangreich sind und entsprechend Zeit benötigen.

gen. Zur schnellen Berechnung des Challenge- bzw. des Response-signales werden speziell für diesen Zweck entwickelte anwenderspezifische integrierte Schaltkreise (ASIC) eingesetzt, welche die Challenge- bzw. Responseberechnung in weniger als drei Millisekunden durchführen. Damit kann das Auslösen der Zuordnungsprüfung durch Betätigen des Türgriffes eines Fahrzeuges erfolgen, so daß das Öffnen der Tür nur möglich ist, wenn die Fernbedienung als zum Fahrzeug gehörig verifiziert wurde. Der Benutzer bemerkt den Zuordnungsvorgang nicht. Die vorgenannten ASICs erfüllen ihre Funktion gut, sind allerdings in der Herstellung vergleichsweise teuer.

Es ist Aufgabe der Erfindung, ein Verfahren zum Zuordnen einer Fernbedienung zu einer Basisstation anzugeben, welches eine schnelle Durchführung einer Zuordnungsprüfung, insbesondere eine schnelle Durchführung einer Verifikationskommunikation gestattet.

Die Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen des Hauptanspruchs. Das erfindungsgemäße Verfahren ist leicht als Programm in dem in Basisstation bzw. Fernbedienung ohnehin vorhandenen Mikroprozessor realisierbar, und macht die Bereitstellung eines ASIC überflüssig. Es gewährleistet dabei dieselbe Sicherheit wie bei Verwendung eines ASICs. Vorteilhaft läßt sich ein Sicherheitsgewinn realisieren, indem die Geschwindigkeit der Challenge-Response-Berechnung gezielt gesteuert wird, wenn der Challenge-Response-Dialog mehrfach unmittelbar hintereinander durchgeführt wird.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend unter Bezugnahme auf die Zeichnung näher erläutert.

Zeichnung

5

Es zeigen Figur 1 ein Blockdiagramm einer Zugangsvorrichtung, Figur 2 ein Flußdiagramm zur Veranschaulichung ihres Betriebes.

10

Beschreibung

15

Figur 1 zeigt eine Basisstation 10, die Teil eines Gerätes oder Gegenstandes sein kann oder einem solchen fest zugeordnet ist. Beispielsweise kann die Basisstation Teil der Zugangskontrolleinrichtung eines Gebäudes oder eines Kraftfahrzeuges sein. Weiterer Bestandteil der in Figur 1 gezeigten Zugangsvorrichtung ist eine im folgenden Fernbedienung genannte Betätigseinrichtung 20, welche der Basisstation funktionell über eine Signalübertragungsstrecke 30 berührungslos zugeordnet ist. Die Fernbedienung kann insbesondere ein Transponder sein. Über nicht dargestellte Wirkverbindungen wirkt die Basisstation 10 auf die technische Einrichtung ein, deren Teil oder der sie zugeordnet ist. Bei Verwendung in einem Kraftfahrzeug kontrolliert sie beispielsweise den Zugang in das Fahrzeug oder dessen Inbetriebnahme.

20

25

Bestandteil der Basisstation 10 ist ein Mikroprozessor 13, welcher den Betrieb der Basisstation 10 kontrolliert, dazu insbesondere die Ausgabe von Signalen veranlaßt und eingehende Signale auswertet. Mit dem Mikroprozessor verbunden ist eine Sende-/Empfangseinrichtung 11 zur Abgabe bzw. Entgegennahme von über die Signalübertragungsstrecke 30 berührungslos übertragenen Signalen. Dem Mikroprozessor 13 ist weiterhin ein Speicher 14 zugeordnet. Darin befinden sich Zuordnungsinformationen, aufgrund derer die Basisstation 10

30

35

zuordnete Fernbedienungen 20 erkennt. Die Zuordnungs-
informationen sind: eine Seriennummer 15, ein Herstellercode
17, ein kryptischer Schlüsselcode 31, ein Verzeichnis 16 mit
Informationen über die der Basisstation 10 zugeordneten
Fernbedienungen 20, sowie eine Zufallszahl 18. Die Serien-
nummer 15 ist charakteristisch für einander zugeordnete Ba-

5 sisstationen 10 und Fernbedienungen 20. Sie wird vom Her-
steller der technischen Einrichtung festgelegt, der die Ba-
sisstation 10 bzw. die Fernbedienungen 20 zugeordnet sind.

10 Bei Verwendung in Kraftfahrzeugen etwa kann die Festlegung
durch den Fahrzeugherrsteller erfolgen. Der Herstellercode 17
bezeichnet das zugehörige Gerät, d.h. die Basisstation 10
eindeutig. Er wird vom Hersteller der Basisstation vergeben
und ist unveränderbar. Das Verzeichnis 16 beinhaltet für je-
15 de zugeordnete Fernbedienung 20 einen Datensatz 16a, 16b,
16c, welcher jeweils die Gruppennummer 25 einer Fernbedie-
nung 20, ihren Herstellercode 27, eine Zufallszahl sowie ei-
ne Soll-Response enthält. Die Gruppennummern 25 unterschei-
den dabei die einer Basisstation 10 zugeordneten Fernbedie-
nungen mit gleichen Seriennummern, der jeweils zugehörige
20 Herstellercode 27 dient in Verbindung mit dem kryptischen
Schlüsselcode 31 und der Zufallszahl 18, die vom Mikropro-
zessor 13 erzeugt wird, zur Bildung der Soll-Response. Der
kryptische Schlüsselcode 31 wird vorzugsweise ebenfalls vom
Hersteller der zugehörigen technischen Einrichtung, etwa ei-
25 nem Fahrzeugherrsteller festgelegt. Jeweils ein ganzer Daten-
satz 16a, 16b, 16c erlaubt die Verifizierung einer zugehöri-
gen Fernbedienung 20.

30 Die Fernbedienung verfügt über eine zur basisstationsseiti-
gen Sende-/Empfangseinrichtung 11 korrespondierende Sende-
/Empfangseinrichtung 21, zum Empfang von der Basisstation 10
abgegebenen Signalen bzw. zur Abgabe von Signalen an die Ba-
sisstation 10. Analog zur Basisstation ist der Sende-
35 /Empfangseinrichtung 21 ein Mikroprozessor 23 nachgeschaltet

welcher den Betrieb der Fernbedienung 20 steuert, wobei er
besonders die Auswertung der über die Sende-
/Empfangseinrichtung 22 eingehenden Signale vornimmt, abhän-
gig von den Ergebnissen Folgemaßnahmen einleitet und die
Ausgabe von Ausgangssignalen überwacht. Dem Mikroprozessor
23 zugeordnet ist eine Speichereinheit 24, worin Zuordnun-
ginformationen zur Zuordnung der Fernbedienung 20 zu einer
Basisstation 10 abgelegt sind. Gespeichert sind dazu - ana-
log zu Basisstation 10 - eine Seriennummer 15, eine Gruppen-
nummer 25, ein Herstellercode 27 sowie ein kryptischer
Schlüsselcode 31. Die Bedeutung der Speicherinhalte ent-
spricht jeweils der Bedeutung der gleichartigen Speicherin-
halte im Speicher 14 der Basisstation 10. Der Herstellercode
ist durch den Hersteller der Fernbedienung 20 vergeben und
bezeichnet sie eindeutig. Die Seriennummer 15 ist ein für
die aus Basisstation 10 und zugehörigen Fernbedienungen 20
bestehende Gesamtvorrichtung charakteristischer Code und
identisch mit dem Speicher 14 der Basisstation 10 enthalte-
nen Seriennummer. Die Gruppennummer 25 unterscheidet die sel-
be Seriennummer 15 aufweisende Fernbedienungen 20 voneinan-
der. Sie wird bei der Nutzung der Gesamtvorrichtung durch
den Anwender festgelegt. Der kryptische Schlüsselcode 31
wird durch den Hersteller der Basisstation 10 zugehöri-
gen technischen Einrichtung festgelegt und ist identisch mit
dem in der Basisstation vorhandenen. In Verbindung mit dem
Herstellercode 27 und dem von der Basisstation 10 über die
Signalübertragungsstrecke 30 zugeführten Challengesignal di-
net er zur Verifikation der Zugehörigkeit zu einer Basissta-
tion 10.

30

Zwischen Basisstation 10 und Fernbedienungen 20 besteht eine
Signalübertragungsstrecke zur Übertragung berührungslos
übertragbarer Signale zwischen der fernbedienungsseitigen
Sende-/Empfangseinrichtung 21 und der basisstationsseitigen
35 Sende-/Empfangseinrichtung 11. Von der basisstationsseitigen

Sende-/Empfangseinrichtung 11 ausgehende Signale erreichen dabei alle innerhalb ihrer Reichweite befindlichen Fernbedienungen 20. Als Signale werden zweckmäßig Infrarot-/oder Hochfrequenzsignale verwendet.

5

Einer Basisstation 10 können mehrere Fernbedienungen 20 zugeordnet sein. Alle Fernbedienungen 20 und die Basisstation 10 verfügen in ihren Speichern 14, 24 über eine identische Seriennummer 15 und verwenden bei der Verifizierung einen kryptischen Schlüsselcode 31. Die einzelnen Fernbedienungen 20 unterscheiden sich durch ihre Gruppennummern 25 und ihre Herstellercodes 27.

10

Anhand Figur 2 wird nachfolgend der Betrieb der in Figur 1 wiedergegebenen Vorrichtung erläutert. Den Ablaufschritten ist dabei jeweils ein Buchstabe B bzw. F vorangestellt, der angibt, ob der zugehörige Ablaufschritt in der Basisstation 10: B oder in einer Fernbedienung 20: F stattfindet.

15

20

Der Zuordnungsvorgang wird durch die Betätigung eines nicht dargestellten mechanischen, elektrischen oder elektrooptischen Auslösemechanismus durch einen Benutzer ausgelöst, Schritt 100. Bei Anwendung in einem Kraftfahrzeug kann der Auslösemechanismus insbesondere im Betätigen des Türgriffes bestehen.

25

Aufgrund eines beim Auslösen abgegebenen Signales setzt der Mikroprozessor 13 der Basisstation 10 zunächst einen internen Zähler A auf den Wert 0, Schritt 102. Sodann lädt er aus dem Speicher 14 die Zufallszahl 18, welche anschließend das im folgenden „Challenge“-Signal genannte Aktivierungssignal bildet, und die im folgenden „Soll-Response“-Signale genannten, erwarteten Antwortsignale 16a, 16b, 16c für alle der Basisstation 10 zugeordneten Fernbedienungen 20, Schritt 104. Darauf erhöht er den Zähler A um 1, Schritt 106. Nach-

30

35

folgend leitet der Mikroprozessor 13 die Abgabe eines Suchsignales durch die Sende-/Empfangseinrichtung 11 ein, Schritt 108. Das Suchsignal beinhaltet neben einer Start- und Synchronisationsinformation insbesondere die im Speicher 14 abgelegte Seriennummer 15. Es ist zweckmäßig unverschlüsselt und wird von allen innerhalb der Reichweite der Signalübertragungsstrecke 30 befindlichen Fernbedienungen 20 über deren Sende-/Empfangseinrichtungen 21 empfangen.

Ihre Mikroprozessoren 23 überprüfen bei Eingang eines Suchsignales, ob die mit dem Suchsignal übertragene Seriennummer 15 mit der im Speicher 24 der Fernbedienung 20 abgelegten, als Referenzsignal dienenden Seriennummer übereinstimmt. Bei Nichtübereinstimmung nimmt die Fernbedienung 20 an der weiteren Zugehörigkeitsprüfung nicht mehr teil. Bei Übereinstimmung der miteinander verglichenen Signale veranlaßt der Mikroprozessor 23 eine Antwort in Form eines Kontaktsignals, Schritt 112. Als Kontaktsignal dient ein kurzes, einfach aufgebautes Signal, beispielsweise die Gruppennummer 25 der jeweiligen Fernbedienung 20 in bitcodierter Form. Zweckmäßig ist das Kontaktsignal wie das Suchsignal unverschlüsselt. Die Aussendung des Kontaktsignales veranlaßt der Mikroprozessor 24 nach Ablauf einer für die Fernbedienung 20 charakteristischen, durch die Gruppennummer 25 bestimmten Zeitspanne ab dem Eingang des Suchsignales. Sie erfolgt dann in einem Zeitfenster mit vorbestimmter Länge. Die Aussendung ist so bemessen, daß ein sicheres Zuordnen des Kontaktsignals zu dem Zeitfenster sowohl für die Fernbedienung 20 wie für die Basisstation 10 möglich ist.

Durch Prüfen, in welchen Zeitfenstern Kontaktsignale eingegangen sind, stellt nun der Mikroprozessor 13 der Basisstation 10 fest, welche Fernbedienungen 20 mit welchen Gruppennummern anwesend sind, Schritt 114. Wird keine anwesende Fernbedienung 20 ermittelt, prüft der Mikroprozessor 13 den

Wert des Zählers A, Schritt 116. Ist er kleiner als ein vor-
gegebener Bezugswert, beispielsweise 5, veranlaßt er unmit-
telbar erneut die Aussendung eines Suchsignales und wieder-
holt das Verfahren ab Schritt 108 fortlaufend. Wird der Be-
5 zugswert überschritten, bricht der Mikroprozessor 13 die Zu-
gehörigkeitsprüfung ab, Schritt 117. Ergab die Prüfung im
Schritt 114, daß wenigstens eine Fernbedienung 20 anwesend
ist, wählt der Mikroprozessor 13 unter den anwesenden Fern-
bedienungen 20 eine aus, mit welcher er nachfolgend eine Zu-
10 gehörigkeitsprüfung durchführt, Schritt 118. Nach Auswahl
einer Fernbedienung zählt er einen zweiten internen Zähler B
um eine Stufe nach oben, Schritt 120. Darauf veranlaßt der
Mikroprozessor 13 die Aussendung eines nachfolgend Challen-
ge-Signales über die Sende-/Empfangseinrichtung 11. Als
15 Challenge-Signal dient die im Speicher 14 abgelegte Zufalls-
zahl 18.

Die ausgewählte Fernbedienung 20 empfängt über ihre Sende-
/Empfangseinrichtung 21 das Challenge-Signal und bildet dar-
20 aus durch Verknüpfung mit dem Herstellercode 27 und dem
kryptischen Schlüsselcode 31 ein „Response“-Signal, welches
sie als Antwortsignal an die Basisstation 10 zurückschickt,
Schritt 124.

25 Deren Mikroprozessor 13 vergleicht nach Erhalt das von der
Fernbedienung 20 rückgesandte Response-Signal mit den zuvor
im Schritt 104 geladenen Soll-Response-Signal 16a, 16, 16c
der ausgewählten Fernbedienung 20, Schritt 126. Stimmen
der ausgewählten Fernbedienung 20, Schritt 126. Stimmen
30 Soll-Response-Signal und Response-Signal überein, setzt der
Mikroprozessor 13 den internen Zähler B auf den Wert 0 zu-
rück, Schritt 132 und veranlaßt die Ausgabe eines Freigabe-
signals, welches beispielsweise den Zugang zu einem Kraft-
fahrzeug und/oder dessen Betrieb ermöglicht, Schritt 134.
Anschließend bestimmt der Mikroprozessor 13 eine Zufallszahl
35 18 und ermittelt damit für jede im Verzeichnis 16 eingetra-

gene Gruppennummer 25 ein neues Soll-Response-Signal, Schritt 136. Mit der Zufallszahl 18 und den neu gebildeten Soll-Response-Signalen belegt er die Speicherplätze 16a, 16b, 16c und 18 sodann neu. Die neuen Speicherinhalte dienen als Grundlage für die Zuordnungsprüfung im Anschluß an den nächsten erneuten Auslösevorgang. Mit dem Neubeschreiben der Speicherinhalte 16 und 18 ist der Zugehörigkeitsprüf vorgang beendet, Schritt 138.

Ergibt die Prüfung im Schritt 126, daß das von der Fernbedienung 20 zurückgesandte Response-Signal nicht mit dem vom Prozessor geladenen Soll-Response-Signal 16a, 16b, 16c übereinstimmt, setzt der Mikroprozessor 13 den internen Zähler B um eine Stufe hoch, Schritt 128. Sodann prüft er, ob der Inhalt des Zählers B einen vorgegebenen Grenzwert, zum Beispiel den Wert 3 überschreitet, Schritt 130. Ist das der Fall, ermittelt der Mikroprozessor 13 gemäß Schritt 136 eine neue Zufallszahl 18 und neue Soll-Response-Signale 16a, 16b, 16c mit denen er die entsprechenden Speicherinhalte im Speicher 14 überschreibt. Danach bricht er den Zuordnungsprüf vorgang ab, Schritt 138.

Ergibt die Prüfung im Schritt 130, daß der dem Zähler B zugeordnete Grenzwert noch nicht überschritten ist, führt der Mikroprozessor 13 ebenfalls eine Neubestimmung der Zufallszahl 18 und der Soll-Response-Signale 16a, 16b, 16c gemäß Schritt 136 durch. Anschließend fährt er jedoch mit der Wiederholung des Schrittes 104 fort und lädt die neubestimmten Speicherinhalte 18 und 16a, 16b, 16c unmittelbar neu, um nachfolgend Schritt 106 auszuführen..

Es kann vorgesehen sein, die Bestimmung einer neuen Zufallszahl und neuer Soll-Responsesignale gemäß Schritt 136 gezielt langsam auszuführen. Da die Neubestimmung bei autorisierter Benutzung erst im Anschluß an die Bestätigung der

Zugehörigkeit und der Ausgabe eines Freigabesignales erfolgt, wirkt sich eine langsame Durchführung des Schrittes 136 für den autorisierten Benutzer nicht aus. Hingegen wird einem Nichtberechtigten das Vortäuschen einer Zugehörigkeit einer Fernbedienung zu einer Basisstation erschwert, selbst wenn es ihm gelingen sollte, die Basisstation durch Nachbilden eines Kontaktsignals zur Abgabe eines Challengesignales an die Fernbedienung zu veranlassen. Durch gezielte Dehnung der Zeit zur Durchführung des Schrittes 136 wird es zudem er-
schwert, ein richtiges Response-Signal durch permutatives
Wiederholen möglicher Response-Signale zu ermitteln.

5

10

18.08.97 Ba/Wt

5

ROBERT BOSCH GMBH, 70442 Stuttgart

10

Ansprüche

15

1. Verfahren zum Zuordnen einer Fernbedienung zu einer Basisstation, wobei die Basisstation (10) ein Suchsignal aussendet (108), die Fernbedienung (20) bei Übereinstimmung des Suchsignales mit einem abgespeicherten Referenzsignal ein Kontaktsignal zurücksendet (112), und die Basisstation (10) daraufhin ein bei jeder Zuordnung veränderliches Aktivierungssignal zur Verifikation der Zugehörigkeit zu der Fernbedienung abgibt (122), dadurch gekennzeichnet, daß das veränderliche Aktivierungssignal bereits vor Aussendung des Suchsignals von der Basisstation festgelegt (136) und für die Zuordnung nur abgerufen wird (104).

20

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß von der Basisstation (10) bereits vor Absetzen des Suchsignals auch das Antwortsignal festgelegt wird (136), mit dem die zugehörige Fernbedienung (20) nach Erhalt des veränderlichen Aktivierungssignales antworten soll.

25

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Festlegung des veränderlichen Aktivierungssignales jeweils nach Abschluß einer erfolgreichen Zuordnung (126, 134) einer Fernbedienung (20) zu einer Basisstation (10) erfolgt.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein neues veränderliches Aktivierungssignal festgelegt wird (136), wenn ein von einer Fernbedienung (20) auf ein Aktivierungssignal hin zurückgesandtes Antwortsignal nicht mit dem in der Basisstation (10) vorbestimmten Sollantwortsignal übereinstimmt.

5
10 5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Suchsignal mehrfach unmittelbar hintereinander ausgesandt wird, wenn auf das vorhergehende Suchsignal ein Kontaktignal nicht eingeht.

15 6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Durchführungszeit bei der Neufestlegung des veränderlichen Aktivierungssignales gegenüber der kürzestmöglichen verlängert wird.

20 7. Basisstation zur Durchführung des Verfahrens nach Anspruch 1, gekennzeichnet durch
- eine Sende-/Empfangseinrichtung (11), welche zur Abgabe von Such- und Aktivierungssignalen sowie zum Empfang von Kontakt- sowie Antwortsignalen von Fernbedienungen (20) ausgebildet ist,
- Mittel (13) zur Veranlassung/Auswertung der über die Sende-/Empfangseinrichtung (11) abzusetzenden/empfangenen Signale,
- sowie eine nichtflüchtige Speichereinheit (14) zur Ablage von feststehenden und veränderlichen Zuordnungsinformationen (15, 17, 31, 16, 18), welche der Basisstation (10) wenigstens eine Fernbedienung (20) zuordnen und die Prüfung der Zugehörigkeit erlauben.

30 35 8. Basisstation nach Anspruch 7, dadurch gekennzeichnet, daß die nichtflüchtige Speichereinheit (14) als genau einmal programmierbares Speichermedium ausgeführt ist.

9. Fernbedienung zur Durchführung des Verfahrens nach Anspruch 1, gekennzeichnet durch

- eine Sende-/Empfangseinrichtung (21), welche zum Empfang von Such- und Aktierungssignalen, sowie zur Abgabe von Kontakt- und Antwortsignalen ausgebildet ist,

5 - Mittel (23) zur Auswertung/Veranlassung empfänger/abzusetzender Signale,

- sowie eine nichtflüchtige Speichereinheit (24) zur Ablage von Zuordnungsinformationen (15, 25, 27, 31), welche die 10 Fernbedienung (20) einer Basisstation (10) zuordnen.

18.08.97 Ba/Wt

5

ROBERT BOSCH GMBH, 70442 Stuttgart

10

Vefahren zum Zuordnen einer Fernbedienung zu einer Basisstation

Zusammenfassung

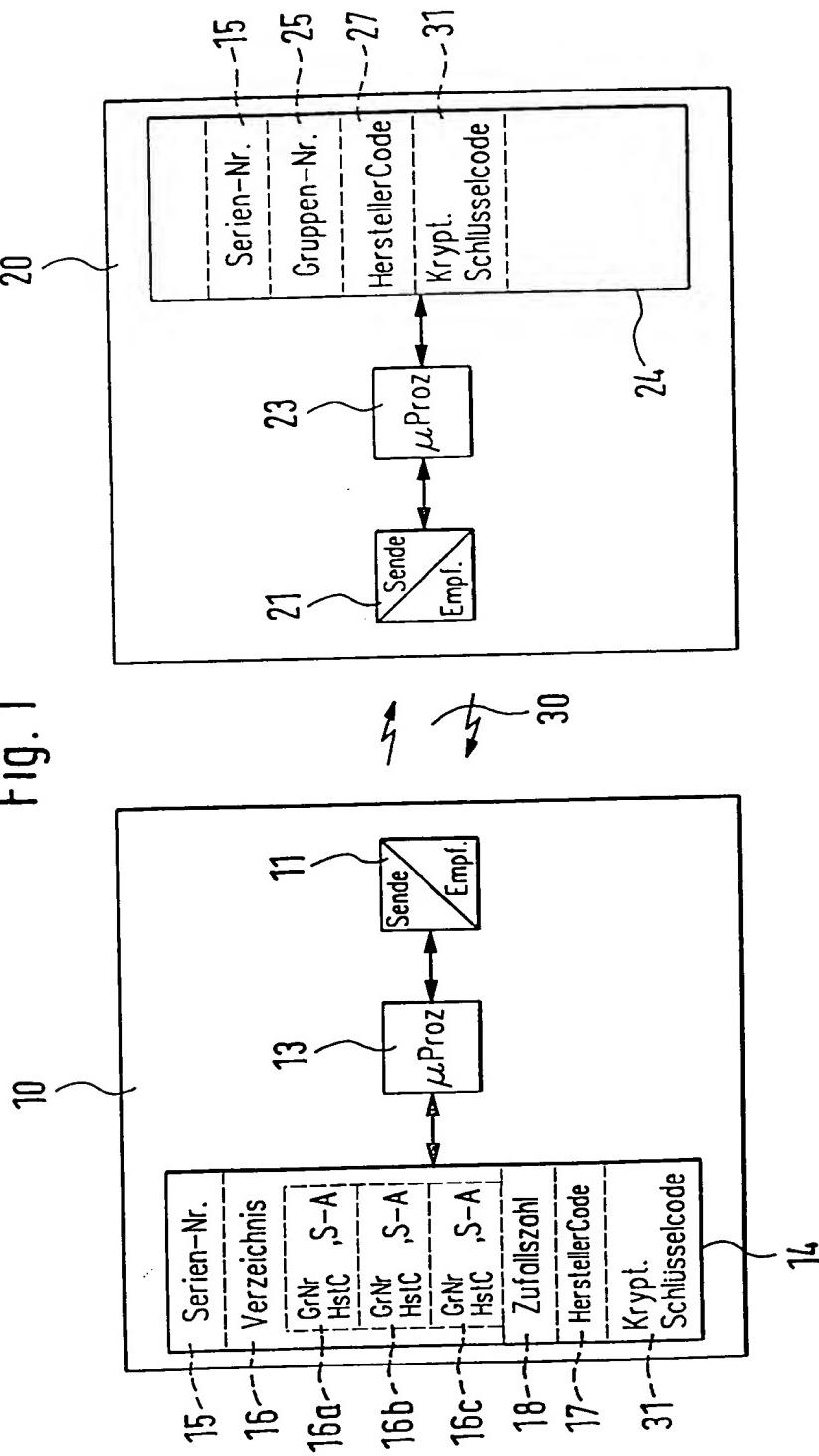
15

Vorgeschlagen wird ein Verfahren zum Zuordnen einer Fernbedienung zu einer Basisstation. Die Basisstation (10) sendet dabei ein Suchsignal aus (108), auf das hin die Fernbedienung (20) bei Übereinstimmung des Suchsignales mit einem abgespeicherten Referenzsignal ein Kontaktsignal zurücksendet (112). Nach dessen Eingang setzt die Basisstation (10) ein bei jeder Zuordnung veränderliches Aktivierungssignal zur Verifikation der Zugehörigkeit zu der Fernbedienung (20) ab (122). Das veränderliche Aktivierungssignal wurde dabei bereits vor Aussendung des Suchsignales von der Basisstation festgelegt (136), gespeichert, und wird für die Zuordnung nur abgerufen (104).

30

(Figur 2)

Fig. 1



2 / 2

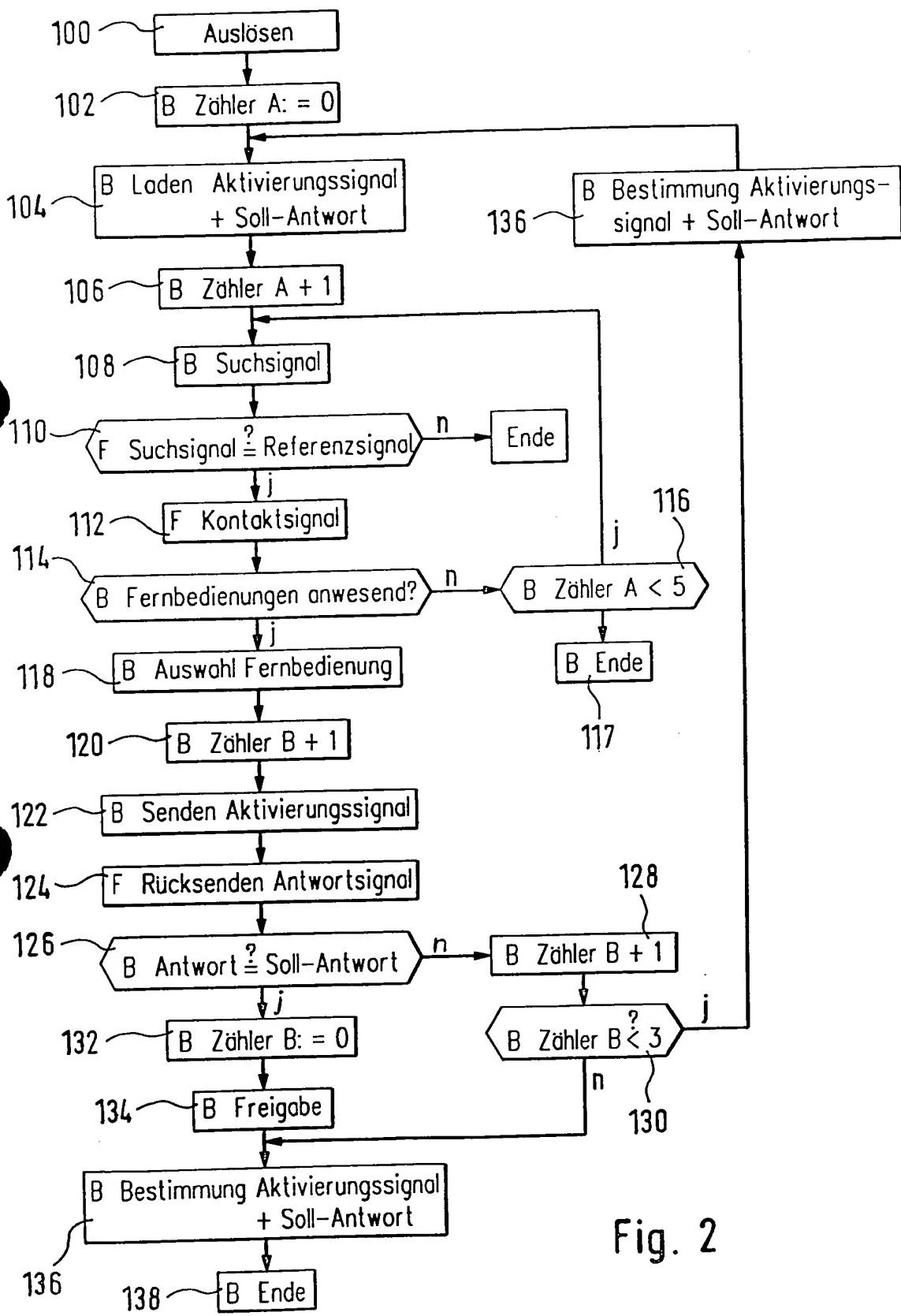


Fig. 2

BUNDESREPUBLIK DEUTSCHLAND

DE 98 12808

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)



REC'D 23 DEC. 1998
WIPO PCT

Bescheinigung

Die ROBERT BOSCH GMBH in Stuttgart/Deutschland hat eine
Patentanmeldung unter der Bezeichnung

"Verfahren zum Zuordnen einer Fernbedienung zu
einer Basisstation"

am 10. September 1998 beim Deutschen Patentamt eingereicht
und erklärt, daß sie dafür die Innere Priorität der
Anmeldung in der Bundesrepublik Deutschland vom
26. September 1997, Aktenzeichen 197 42 495.3, in Anspruch
nimmt.

Die angehefteten Stücke sind eine richtige und genaue
Wiedergabe der ursprünglichen Unterlagen dieser Patent-
anmeldung.

Die Anmeldung hat im Deutschen Patentamt vorläufig das Symbol
G 08 C 17/02 der Internationalen Patentklassifikation erhalten.

München, den 9. Oktober 1998
Der Präsident des Deutschen Patentamts
Im Auftrag

Aktenzeichen: 198 41 514.1

Ebert

10.09.98 Ba/Wt

5

ROBERT BOSCH GMBH, 70442 Stuttgart

10

Vefahren zum Zuordnen einer Fernbedienung zu einer
Basisstation

Stand der Technik

15

Die Erfindung geht aus von einem Verfahren nach der Gattung des Hauptanspruchs, wie es in der Deutschen Patentanmeldung AZ: 196 45 769.6 beschrieben ist. Danach erfolgt die Zuordnung einer Fernbedienung zu einer in einem Kraftfahrzeug angeordneten Basisstation, indem letztere ein Suchsignal absetzt, worauf im Reichweitenbereich des Suchsignales befindliche Fernbedienungen durch Rücksenden eines Kontakt signales zu für die Fernbedienungen charakteristischen Zeitpunkten antworten. Durch Auswertung der Eingangszeitpunkte der Kontakt signalrückmeldungen ermittelt die Basisstation die anwesenden Fernbedienungen. Eine davon wählt sie aus, und führt mit ihr eine „Challenge-Response“ -Verifikation durch. Weil eine eindeutige Fernbedienungserkennung bereits durch Austausch von nur einem Signal möglich ist, und das Signal, da es nicht sicherheitsrelevant ist, einfach aufgebaut sein kann, erfolgt die gesamte Erkennung sehr schnell. Bestimmend für die Zuordnungsgeschwindigkeit ist daher vor allem die nachfolgende Challenge-Response-Verifikation. Sie basiert auf der Durchführung von sicherheitsrelevanten Rechenoperationen, die umfangreich sind und entsprechend Zeit benötigen.

30

35

gen. Zur schnellen Berechnung des Challenge- bzw. des Response signales werden speziell für diesen Zweck entwickelte anwenderspezifische integrierte Schaltkreise (ASIC) eingesetzt, welche die Challenge- bzw. Responseberechnung in weniger als drei Millisekunden durchführen. Damit kann das Auslösen der Zuordnungsprüfung durch Betätigen des Türgriffes eines Fahrzeuges erfolgen, so daß das Öffnen der Tür nur möglich ist, wenn die Fernbedienung als zum Fahrzeug gehörig verifiziert wurde. Der Benutzer bemerkt den Zuordnungsvorgang nicht. Die vorgenannten ASICs erfüllen ihre Funktion gut, sind allerdings in der Herstellung vergleichsweise teuer.

Es ist Aufgabe der Erfindung, ein Verfahren zum Zuordnen einer Fernbedienung zu einer Basisstation anzugeben, welches eine schnelle Durchführung einer Zuordnungsprüfung, insbesondere eine schnelle Durchführung einer Verifikationskommunikation gestattet.

Die Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen des Hauptanspruchs. Das erfindungsgemäße Verfahren ist leicht als Programm in dem in Basisstation bzw. Fernbedienung ohnehin vorhandenen Mikroprozessor realisierbar, und macht die Bereitstellung eines ASIC überflüssig. Es gewährleistet dabei dieselbe Sicherheit wie bei Verwendung eines ASICs. Vorteilhaft läßt sich ein Sicherheitsgewinn realisieren, indem die Geschwindigkeit der Challenge-Response-Berechnung gezielt gesteuert wird, wenn der Challenge-Response-Dialog mehrfach unmittelbar hintereinander durchgeführt wird.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend unter Bezugnahme auf die Zeichnung näher erläutert.

Zeichnung

5

Es zeigen Figur 1 ein Blockdiagramm einer Zugangsvorrichtung, Figur 2 ein Flußdiagramm zur Veranschaulichung ihres Betriebes.

10

Beschreibung

15

Figur 1 zeigt eine Basisstation 10, die Teil eines Gerätes oder Gegenstandes sein kann oder einem solchen fest zugeordnet ist. Beispielsweise kann die Basisstation Teil der Zugangskontrolleinrichtung eines Gebäudes oder eines Kraftfahrzeuges sein. Weiterer Bestandteil der in Figur 1 gezeigten Zugangsvorrichtung ist eine im folgenden Fernbedienung genannte Betätigungsseinrichtung 20, welche der Basisstation funktionell über eine Signalübertragungsstrecke 30 berührungslos zugeordnet ist. Die Fernbedienung kann insbesondere ein Transponder sein. Über nicht dargestellte Wirkverbindungen wirkt die Basisstation 10 auf die technische Einrichtung ein, deren Teil oder der sie zugeordnet ist. Bei Verwendung in einem Kraftfahrzeug kontrolliert sie beispielsweise den Zugang in das Fahrzeug oder dessen Inbetriebnahme.

20

30

35

Bestandteil der Basisstation 10 ist ein Mikroprozessor 13, welcher den Betrieb der Basisstation 10 kontrolliert, dazu insbesondere die Ausgabe von Signalen veranlaßt und eingehende Signale auswertet. Mit dem Mikroprozessor verbunden ist eine Sende-/Empfangseinrichtung 11 zur Abgabe bzw. Entgegennahme von über die Signalübertragungsstrecke 30 berührungslos übertragenen Signalen. Dem Mikroprozessor 13 ist weiterhin ein Speicher 14 zugeordnet. Darin befinden sich Zuordnungsinformationen, aufgrund derer die Basisstation 10

zuordnete Fernbedienungen 20 erkennt. Die Zuordnungsinformationen sind: eine Seriennummer 15, ein Herstellercode 17, ein kryptischer Schlüsselcode 31, ein Verzeichnis 16 mit Informationen über die der Basisstation 10 zugeordneten Fernbedienungen 20, sowie eine Zufallszahl 18. Die Seriennummer 15 ist charakteristisch für einander zugeordnete Basisstationen 10 und Fernbedienungen 20. Sie wird vom Hersteller der technischen Einrichtung festgelegt, der die Basisstation 10 bzw. die Fernbedienungen 20 zugeordnet sind. Bei Verwendung in Kraftfahrzeugen etwa kann die Festlegung durch den Fahrzeugherrsteller erfolgen. Der Herstellercode 17 bezeichnet das zugehörige Gerät, d.h. die Basisstation 10 eindeutig. Er wird vom Hersteller der Basisstation vergeben und ist unveränderbar. Das Verzeichnis 16 beinhaltet für jede zugeordnete Fernbedienung 20 einen Datensatz 16a, 16b, 16c, welcher jeweils die Gruppennummer 25 einer Fernbedienung 20, ihren Herstellercode 27, eine Zufallszahl sowie eine Soll-Response enthält. Die Gruppennummern 25 unterscheiden dabei die einer Basisstation 10 zugeordneten Fernbedienungen mit gleichen Seriennummern, der jeweils zugehörige Herstellercode 27 dient in Verbindung mit dem kryptischen Schlüsselcode 31 und der Zufallszahl 18, die vom Mikroprozessor 13 erzeugt wird, zur Bildung der Soll-Response. Der kryptische Schlüsselcode 31 wird vorzugsweise ebenfalls vom Hersteller der zugehörigen technischen Einrichtung, etwa einem Fahrzeugherrsteller festgelegt. Jeweils ein ganzer Datensatz 16a, 16b, 16c erlaubt die Verifizierung einer zugehörigen Fernbedienung 20.

Die Fernbedienung verfügt über eine zur basisstationsseitigen Sende-/Empfangseinrichtung 11 korrespondierende Sende-/Empfangseinrichtung 21, zum Empfang von der Basisstation 10 abgegebenen Signalen bzw. zur Abgabe von Signalen an die Basisstation 10. Analog zur Basisstation ist der Sende-/Empfangseinrichtung 21 ein Mikroprozessor 23 nachgeschaltet

welcher den Betrieb der Fernbedienung 20 steuert, wobei er
besonders die Auswertung der über die Sende-
/Empfangseinrichtung 22 eingehenden Signale vornimmt, abhän-
gig von den Ergebnissen Folgemaßnahmen einleitet und die
Ausgabe von Ausgangssignalen überwacht. Dem Mikroprozessor
23 zugeordnet ist eine Speichereinheit 24, worin Zuordnun-
ginformationen zur Zuordnung der Fernbedienung 20 zu einer
Basisstation 10 abgelegt sind. Gespeichert sind dazu - ana-
log zu Basisstation 10 - eine Seriennummer 15, eine Gruppen-
nummer 25, ein Herstellercode 27 sowie ein kryptischer
Schlüsselcode 31. Die Bedeutung der Speicherinhalte ent-
spricht jeweils der Bedeutung der gleichartigen Speicherin-
halte im Speicher 14 der Basisstation 10. Der Herstellercode
ist durch den Hersteller der Fernbedienung 20 vergeben und
bezeichnet sie eindeutig. Die Seriennummer 15 ist ein für
die aus Basisstation 10 und zugehörigen Fernbedienungen 20
bestehende Gesamtvorrichtung charakteristischer Code und
identisch mit dem Speicher 14 der Basisstation 10 enthalte-
nen Seriennummer. Die Gruppennummer 25 unterscheidet die sel-
be Seriennummer 15 aufweisende Fernbedienungen 20 voneinan-
der. Sie wird bei der Nutzung der Gesamtvorrichtung durch
den Anwender festgelegt. Der kryptische Schlüsselcode 31
wird durch den Hersteller der Basisstation 10 zugehöri-
gen technischen Einrichtung festgelegt und ist identisch mit
dem in der Basisstation vorhandenen. In Verbindung mit dem
Herstellercode 27 und dem von der Basisstation 10 über die
Signalübertragungsstrecke 30 zugeführten Challengesignal di-
net er zur Verifikation der Zugehörigkeit zu einer Basissta-
tion 10.

Zwischen Basisstation 10 und Fernbedienungen 20 besteht eine
Signalübertragungsstrecke zur Übertragung berührungslos
übertragbarer Signale zwischen der fernbedienungsseitigen
Sende-/Empfangseinrichtung 21 und der basisstationsseitigen
Sende-/Empfangseinrichtung 11. Von der basisstationsseitigen

Sende-/Empfangseinrichtung 11 ausgehende Signale erreichen dabei alle innerhalb ihrer Reichweite befindlichen Fernbedienungen 20. Als Signale werden zweckmäßig Infrarot-/oder Hochfrequenzsignale verwendet.

5

Einer Basisstation 10 können mehrere Fernbedienungen 20 zugeordnet sein. Alle Fernbedienungen 20 und die Basisstation 10 verfügen in ihren Speichern 14, 24 über eine identische Seriennummer 15 und verwenden bei der Verifizierung einen kryptischen Schlüsselcode 31. Die einzelnen Fernbedienungen 20 unterscheiden sich durch ihre Gruppennummern 25 und ihre Herstellercodes 27.

10

Anhand Figur 2 wird nachfolgend der Betrieb der in Figur 1 wiedergegebenen Vorrichtung erläutert. Den Ablaufschritten ist dabei jeweils ein Buchstabe B bzw. F vorangestellt, der angibt, ob der zugehörige Ablaufschritt in der Basisstation 10: B oder in einer Fernbedienung 20: F stattfindet.

15

Der Zuordnungsvorgang wird durch die Betätigung eines nicht dargestellten mechanischen, elektrischen oder elektrooptischen Auslösemechanismus durch einen Benutzer ausgelöst, Schritt 100. Bei Anwendung in einem Kraftfahrzeug kann der Auslösemechanismus insbesondere im Betätigen des Türgriffes bestehen.

20

Aufgrund eines beim Auslösen abgegebenen Signales setzt der Mikroprozessor 13 der Basisstation 10 zunächst einen internen Zähler A auf den Wert 0, Schritt 102. Sodann lädt er aus dem Speicher 14 die Zufallszahl 18, welche anschließend das im folgenden „Challenge“ -Signal genannte Aktivierungssignal bildet, und die im folgenden „Soll-Response“ -Signale genannten, erwarteten Antwortsignale 16a, 16b, 16c für alle der Basisstation 10 zugeordneten Fernbedienungen 20, Schritt 104. Darauf erhöht er den Zähler A um 1, Schritt

30

35

106. Nachfolgend leitet der Mikroprozessor 13 die Abgabe eines Suchsignales durch die Sende-/Empfangseinrichtung 11 ein, Schritt 108. Das Suchsignal beinhaltet neben einer Start- und Synchronisationsinformation insbesondere die im Speicher 14 abgelegte Seriennummer 15. Es ist zweckmäßig unverschlüsselt und wird von allen innerhalb der Reichweite der Signalübertragungsstrecke 30 befindlichen Fernbedienungen 20 über deren Sende-/Empfangseinrichtungen 21 empfangen.

10 Ihre Mikroprozessoren 23 überprüfen bei Eingang eines Suchsignales, ob die mit dem Suchsignal übertragene Seriennummer 15 mit der im Speicher 24 der Fernbedienung 20 abgelegten, als Referenzsignal dienenden Seriennummer übereinstimmt. Bei Nichtübereinstimmung nimmt die Fernbedienung 20 an der weiteren Zugehörigkeitsprüfung nicht mehr teil. Bei Übereinstimmung der miteinander verglichenen Signale veranlaßt der Mikroprozessor 23 eine Antwort in Form eines Kontaktsignals, Schritt 112. Als Kontaktsignal dient ein kurzes, einfach aufgebautes Signal, beispielsweise die Gruppennummer 25 der jeweiligen Fernbedienung 20 in bitcodierter Form. Zweckmäßig ist das Kontaktsignal wie das Suchsignal unverschlüsselt. Die Aussendung des Kontaktsignales veranlaßt der Mikroprozessor 24 nach Ablauf einer für die Fernbedienung 20 charakteristischen, durch die Gruppennummer 25 bestimmten Zeitspanne ab dem Eingang des Suchsignales. Sie erfolgt dann in einem Zeitfenster mit vorbestimmter Länge. Die Aussendung ist so bemessen, daß ein sicheres Zuordnen des Kontaktsignals zu dem Zeitfenster sowohl für die Fernbedienung 20 wie für die Basisstation 10 möglich ist.

30 Durch Prüfen, in welchen Zeitfenstern Kontaktsignale eingingen sind, stellt nun der Mikroprozessor 13 der Basisstation 10 fest, welche Fernbedienungen 20 mit welchen Gruppennummern anwesend sind, Schritt 114. Wird keine anwesende Fernbedienung 20 ermittelt, prüft der Mikroprozessor 13 den

Wert des Zählers A, Schritt 116. Ist er kleiner als ein vor-
gegebener Bezugswert, beispielsweise 5, veranlaßt er unmit-
telbar erneut die Aussendung eines Suchsignales und wieder-
holt das Verfahren ab Schritt 106 fortlaufend. Wird der Be-
5 zugswert überschritten, bricht der Mikroprozessor 13 die Zu-
gehörigkeitsprüfung ab, Schritt 117. Ergab die Prüfung im
Schritt 114, daß wenigstens eine Fernbedienung 20 anwesend
ist, wählt der Mikroprozessor 13 unter den anwesenden Fern-
bedienungen 20 eine aus, mit welcher er nachfolgend eine Zu-
10 gehörigkeitsprüfung durchführt, Schritt 118. Nach Auswahl
einer Fernbedienung zählt er einen zweiten internen Zähler B
um eine Stufe nach oben, Schritt 120. Darauf veranlaßt der
Mikroprozessor 13 die Aussendung eines nachfolgend Challen-
ge-Signales über die Sende-/Empfangseinrichtung 11. Als
15 Challenge-Signal dient die im Speicher 14 abgelegte Zufalls-
zahl 18.

Die ausgewählte Fernbedienung 20 empfängt über ihre Sende-
/Empfangseinrichtung 21 das Challenge-Signal und bildet dar-
aus durch Verknüpfung mit dem Herstellercode 27 und dem
20 kryptischen Schlüsselcode 31 ein „Response“ -Signal, welches
sie als Antwortsignal an die Basisstation 10 zurückschickt,
kryptischen Schlüsselcode 31 ein „Response“ -Signal, welches
sie als Antwortsignal an die Basisstation 10 zurückschickt,
Schritt 124.

Deren Mikroprozessor 13 vergleicht nach Erhalt das von der
Fernbedienung 20 rückgesandte Response-Signal mit den zuvor
im Schritt 104 geladenen Soll-Response-Signal 16a, 16, 16c
der ausgewählten Fernbedienung 20, Schritt 126. Stimmen
Soll-Response-Signal und Response-Signal überein, setzt der
30 Mikroprozessor 13 den internen Zähler B auf den Wert 0 zu-
rück, Schritt 132 und veranlaßt die Ausgabe eines Freigabe-
signales, welches beispielsweise den Zugang zu einem Kraft-
fahrzeug und/oder dessen Betrieb ermöglicht, Schritt 134.
Anschließend bestimmt der Mikroprozessor 13 eine Zufallszahl
35 18 und ermittelt damit für jede im Verzeichnis 16 eingetra-

gene Gruppennummer 25 ein neues Soll-Response-Signal, Schritt 136. Mit der Zufallszahl 18 und den neu gebildeten Soll-Response-Signalen belegt er die Speicherplätze 16a, 16b, 16c und 18 sodann neu. Die neuen Speicherinhalte dienen 5 als Grundlage für die Zuordnungsprüfung im Anschluß an den nächsten erneuten Auslösevorgang. Mit dem Neubeschreiben der Speicherinhalte 16 und 18 ist der Zugehörigkeitsprüf vorgang beendet, Schritt 138.

10 Ergibt die Prüfung im Schritt 126, daß das von der Fernbedienung 20 zurückgesandte Response-Signal nicht mit dem vom Prozessor geladenen Soll-Response-Signal 16a, 16b, 16c übereinstimmt, setzt der Mikroprozessor 13 den internen Zähler B um eine Stufe hoch, Schritt 128. Sodann prüft er, ob der Inhalt des Zählers B einen vorgegebenen Grenzwert, zum Beispiel den Wert 3 überschreitet, Schritt 130. Ist das der Fall, ermittelt der Mikroprozessor 13 gemäß Schritt 136 eine neue Zufallszahl 18 und neue Soll-Response-Signale 16a, 16b, 16c mit denen er die entsprechenden Speicherinhalte im Speicher 14 überschreibt. Danach bricht er den Zuordnungs- 15 20 prüfvorgang ab, Schritt 138.

Ergibt die Prüfung im Schritt 130, daß der dem Zähler B zugeordnete Grenzwert noch nicht überschritten ist, führt der Mikroprozessor 13 ebenfalls eine Neubestimmung der Zufallszahl 18 und der Soll-Response-Signale 16a, 16b, 16c gemäß Schritt 136 durch. Anschließend fährt er jedoch mit der Wiederholung des Schrittes 104 fort und lädt die neubestimmten Speicherinhalte 18 und 16a, 16b, 16c unmittelbar neu, um 30 nachfolgend Schritt 106 auszuführen..

Es kann vorgesehen sein, die Bestimmung einer neuen Zufallszahl und neuer Soll-Responsesignale gemäß Schritt 136 gezielt langsam auszuführen. Da die Neubestimmung bei autorisierte 35 r Benutzung erst im Anschluß an die Bestätigung der

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein neues veränderliches Aktivierungssignal festgelegt wird (136), wenn ein von einer Fernbedienung (20) auf ein Aktivierungssignal hin zurückgesandtes Antwortsignal nicht mit dem in der Basisstation (10) vorbestimmten Sollantwortsignal übereinstimmt.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Suchsignal mehrfach unmittelbar hintereinander ausgesandt wird, wenn auf das vorhergehende Suchsignal ein Kontakt signal nicht eingeht.

10 6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Durchführungszeit bei der Neufestlegung des veränderlichen Aktivierungssignales gegenüber der kürzestmöglichen verlängert wird.

15 7. Basisstation zur Durchführung des Verfahrens nach Anspruch 1, gekennzeichnet durch

20 - eine Sende-/Empfangseinrichtung (11), welche zur Abgabe von Such- und Aktivierungssignalen sowie zum Empfang von Kontakt- sowie Antwortsignalen von Fernbedienungen (20) ausgebildet ist,
- Mittel (13) zur Veranlassung/Auswertung der über die Sende-/Empfangseinrichtung (11) abzusetzenden/empfangenen Signale,
- sowie eine nichtflüchtige Speichereinheit (14) zur Ablage von feststehenden und veränderlichen Zuordnungsinformationen (15, 17, 31, 16, 18), welche der Basisstation (10) wenigstens eine Fernbedienung (20) zuordnen und die Prüfung der Zugehörigkeit erlauben.

30 35 8. Basisstation nach Anspruch 7, dadurch gekennzeichnet, daß die nichtflüchtige Speichereinheit (14) als genau einmal programmierbares Speichermedium ausgeführt ist.

9. Fernbedienung zur Durchführung des Verfahrens nach Anspruch 1, gekennzeichnet durch

- eine Sende-/Empfangseinrichtung (21), welche zum Empfang von Such- und Aktierungssignalen, sowie zur Abgabe von Kontakt- und Antwortsignalen ausgebildet ist,
- Mittel (23) zur Auswertung/Veranlassung empfänger/abzusetzender Signale,
- sowie eine nichtflüchtige Speichereinheit (24) zur Ablage von Zuordnungsinformationen (15, 25, 27, 31), welche die Fernbedienung (20) einer Basisstation (10) zuordnen.

5

10

10.09.98 Ba/Wt

5

ROBERT BOSCH GMBH, 70442 Stuttgart

10

Vefahren zum Zuordnen einer Fernbedienung zu einer
Basisstation

Zusammenfassung

15

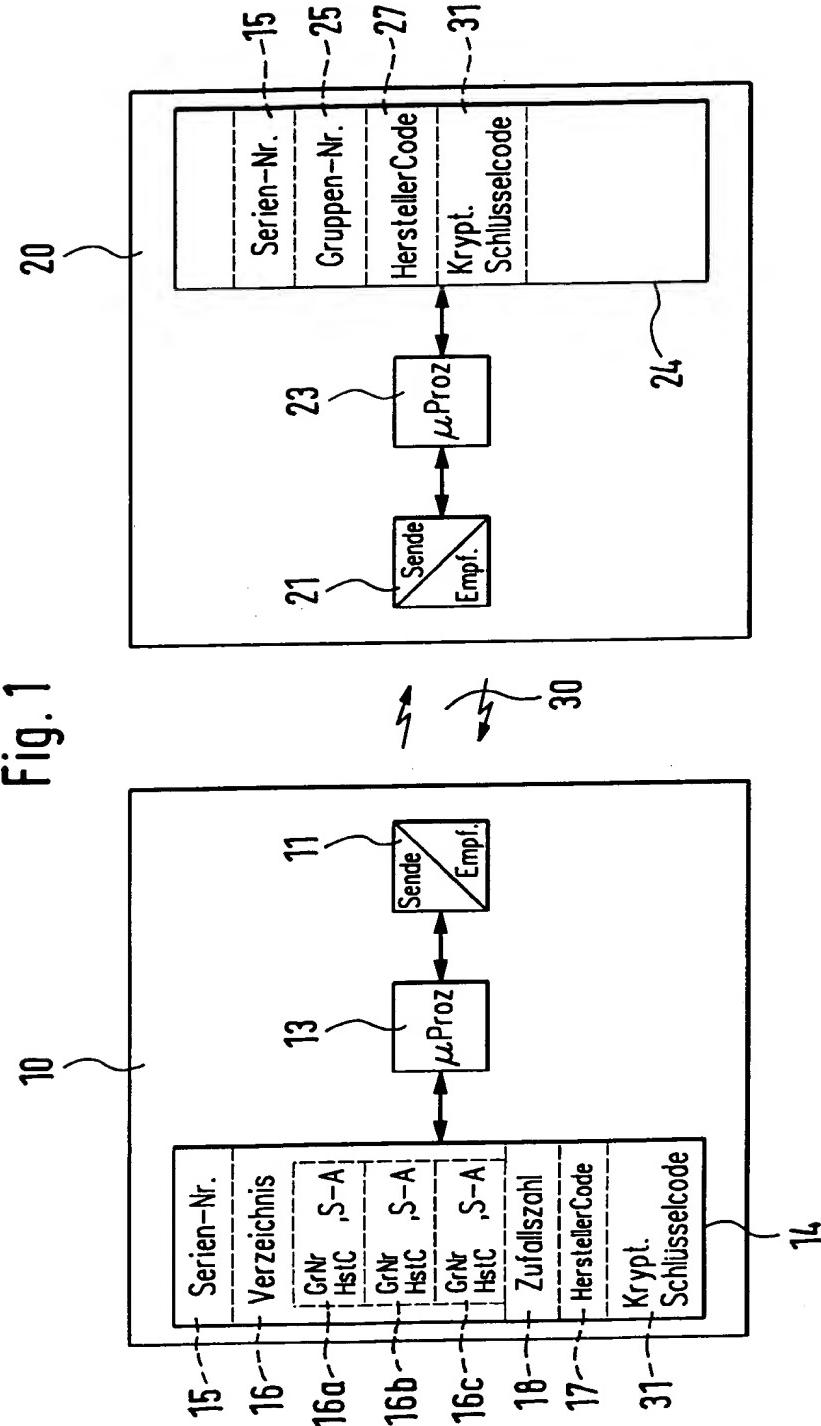
Vorgeschlagen wird ein Verfahren zum Zuordnen einer Fernbedienung zu einer Basisstation. Die Basisstation (10) sendet dabei ein Suchsignal aus (108), auf das hin die Fernbedienung (20) bei Übereinstimmung des Suchsignales mit einem abgespeicherten Referenzsignal ein Kontaktsignal zurücksendet (112). Nach dessen Eingang setzt die Basisstation (10) ein bei jeder Zuordnung veränderliches Aktivierungssignal zur Verifikation der Zugehörigkeit zu der Fernbedienung (20) ab (122). Das veränderliche Aktivierungssignal wurde dabei bereits vor Aussendung des Suchsignales von der Basisstation festgelegt (136), gespeichert, und wird für die Zuordnung nur abgerufen (104).

20

(Figur 2)

30

Fig. 1



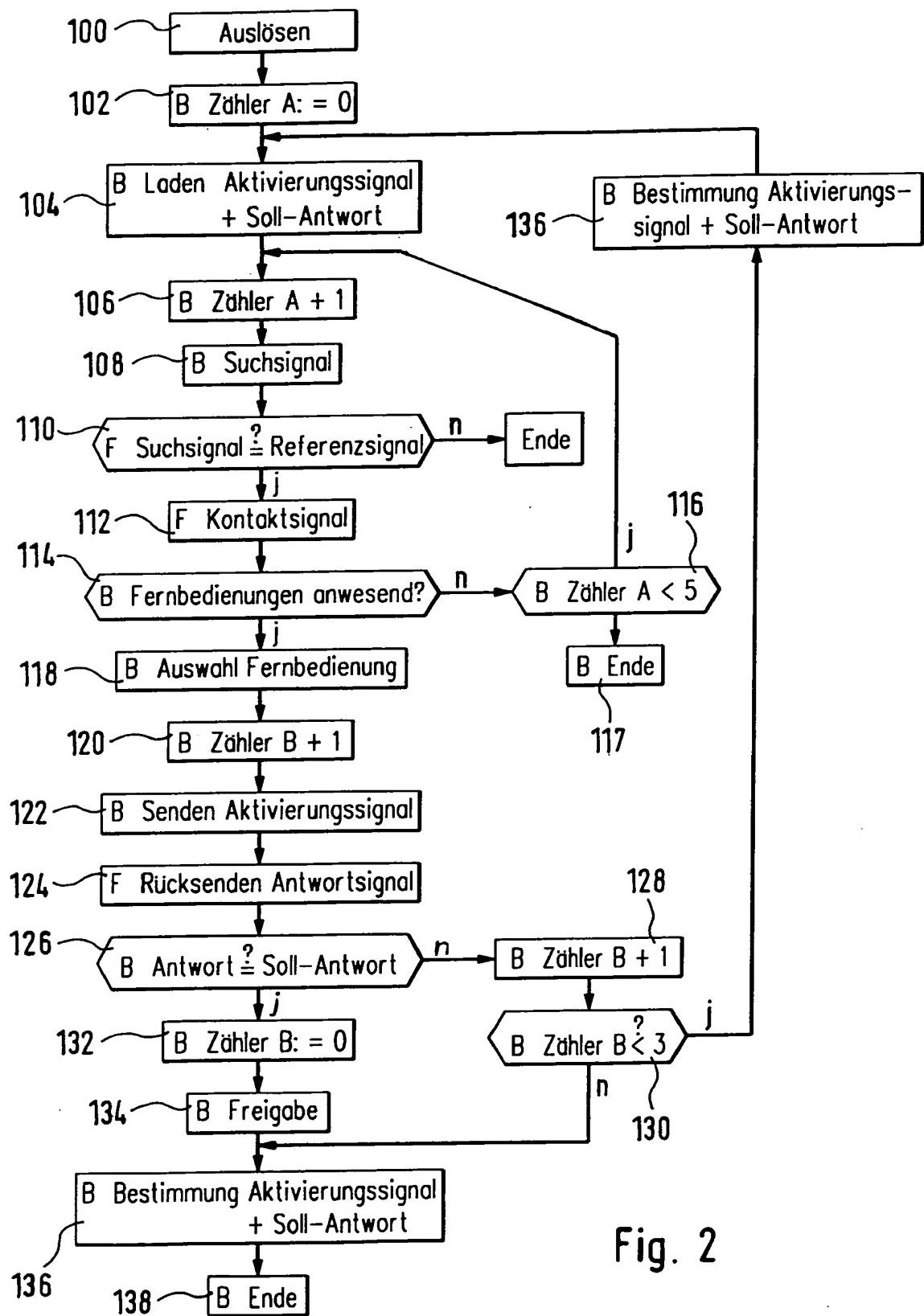


Fig. 2